

UNITED STATES DISTRICT COURT

for the
Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

The Residence, Computers, and Cellular Telephones at
5 Haley Court, Albany, New York, more fully described in
Attachment A

Case No.

15-MJ-458 CFH

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The Residence, Computers, and Cellular Telephones at 5 Haley Court, Albany, New York, more fully described in Attachment A

located in the Northern District of New York, there is now concealed (identify the person or describe the property to be seized):

Evidence and instrumentalities of violations of 18 USC 2251, 18 USC 2422(b), and 18 USC 1470. The items to be seized are detailed in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §2251; 18 U.S.C. §2422(b); and 18 U.S.C. §1470.	Child Exploitation; Enticing a minor to engage in unlawful sexual conduct; transferring obscene images to a minor.

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

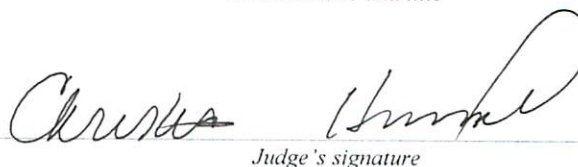
Christ Smith, FBI Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/03/2015

City and state: Albany, New York


Judge's signature

Honorable Christian F. Hummel

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF:

5 Haley Court, Albany, NY 12205

Case No. 15-MJ -458 CFH

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Chris Smith, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Task Force Officer with the Federal Bureau of Investigation, and a police officer with the Colonie, New York Police Department. As a Task Force Officer my responsibilities include the investigation of various federal criminal offenses, including the investigation of crimes involving the sexual exploitation of children. I was a Police Officer in the Colonie Police Department from 2004 until 2009. Since 2009, I have been an Investigator in the Colonie Police Department. In my position, I investigate cases involves child abuse, sexual exploitation, child pornography, and online enticement cases. I was trained at the New York State child abuse and sexual abuse training, and in child exploitation forensic interview training. I am certified by the Federal Bureau of Investigation and the New York State Police in undercover investigations involving child pornography and online enticement. I am a Special Deputy United State Marshal engaged in enforcing the criminal laws, including 18 U.S.C. § 2251, 18 U.S.C. §2422(b), and 18 U.S.C. §1470 and I am authorized by the United States Marshal Service to request a search warrant.

2. I make this affidavit in support of an application for a warrant to search (a) the premises located at 5 Haley Court, Albany, NY 12205 (hereinafter, the "SUBJECT PREMISES") and (b) any computers, computer equipment or computer storage media and

electronic storage media located during the course of said searches, including, but not limited to, an iPhone 4s, Model A1387, iC 579c-e2430a, the phone assigned the number (518) 495-0900, a Samsung Galaxy S5, Model Number SM6360T1, and an HP Laptop Model Number G6-1D60US. A photograph of the SUBJECT PREMISES is attached as Attachment A.

3. As described herein, there is probable cause to believe that Ethan FORDLEY ("FORDLEY") has committed the offenses of: production and attempted production of child pornography, in violation of 18 U.S.C. §2251; using of a means or facility of interstate commerce to induce, persuade and/or entice a minor to engage in unlawful sexual activity, in violation of 18 U.S.C. §2422(b), and using a means or facility of interstate commerce to transfer obscene materials to a minor, in violation of 18 U.S.C. §1470 (the "TARGET OFFENSES"). Further, as described herein, there is probable cause to believe that the SUBJECT PREMISES contains evidence of the TARGET OFFENSES.

4. The items to be seized constitute evidence of the commission of criminal offenses, contraband, fruits of crimes and things otherwise criminally possessed, as well as property designed and intended for use, and that has been used, as a means of committing the TARGET OFFENSES. I request authority to (i) search the entire SUBJECT PREMISES, including the residential dwelling and any computer and computer media located therein, where the items specified in Attachment B may be found; and (ii) seize from the SUBJECT PREMISES any and all items listed in Attachment B as instrumentalities, fruits, and evidence of the TARGET OFFENSES. The evidence described in Attachment B includes evidence maintained in electronic format on any cellular phone, tablet and/or computer device (or other device capable of storing data) within the SUBJECT PREMISES. The methods by which the electronic information will be searched are more fully set forth in the "Computer Evidence" section of this

affidavit.

5. The information set forth in this affidavit is based on an investigation conducted by law enforcement agents, including myself. This affidavit does not contain every fact known to me with respect to this investigation. Rather, it contains those facts that I believe to be necessary to establish probable cause for issuance of the requested warrant to search the SUBJECT PREMISES.

RELEVANT STATUTES

6. Generally, Title 18, United States Code, Section 2251 makes it illegal for a person to entice, persuade, induce, employ, use, or coerce a minor to engage in sexually explicit conduct for the purpose of creating child pornography, or to attempt to do so, where that depiction will be transported in interstate commerce or will be produced utilizing any item that has travelled in interstate commerce.

7. Generally, Title 18, United States Code, Section 2422(b) makes it illegal for a person to use a facility of interstate commerce¹ to attempt to, or to knowingly, persuade, induce or entice, someone younger than eighteen years old to engage in criminal sexual activity.

8. Generally, Title 18, United States Code, Section 1470, makes it illegal for a person to use the mail or any facility of interstate commerce to transfer obscene materials to a minor less than sixteen years old, or to attempt to do so.

9. For purposes of this affidavit, any individual below the age of 18 will be referred to as a “child” or “minor,” and any visual depiction of a child or minor engaging in “sexually

¹ A smartphone, tablet, or computer connected to the Internet is recognized as a “facility of interstate commerce.”

explicit conduct,” as that term is defined in Title 18, United States Code, Section 2256(2)(A), will be referred to as “child pornography.”

THE SUBJECT PREMISES

10. The SUBJECT PREMISES is located at 5 Haley Court, Albany, New York, upon which is a single family ranch style residence light green in color with a two car garage, black shutters and a white door. The SUBJECT PREMISES is more particularly described in Attachment A, hereto.

THE INSTANT INVESTIGATION

11. In late September 2014, thirteen year-old juvenile victim #1 (“JV-1”)² met FORDLEY on an Internet chat site called www.poo.com. The two chatted on the website for approximately two weeks. They also spoke via telephone.

12. JV-1 was interviewed on December 17, 2014, and provided the following information regarding her communications with FORDLEY. When they first met, JV-1 told FORDLEY that she was thirteen (13) years-old. A couple of days later, FORDLEY told JV-1 that he was twenty-three (23) years-old. FORDLEY told JV-1 that he lived with his mother and step-father in Albany, New York. Further, FORDLEY told JV-1 that he was a carpenter and recovering heroin addict. When corresponding on the poo.com website, FORDLEY turned on the webcam feature on at least one occasion and JV-1 was able to see his face. She described him as having dark brown eyes and a square face with stubble.

13. JV-1 provided FORDLEY her home phone number and her cell phone number. FORDLEY and JV-1 engaged in sexually explicit chats (to include more than one discussion

² The identity of JV-1 is known to this affiant.

about sexual intercourse) on the www.poo.com website. FORDLEY was later banned by the moderator of www.poo.com for engaging in sexually explicit chats with JV-1 in approximately the third week of October 2014.

14. JV-1 and FORDLEY also talked on the phone numerous times. When FORDLEY called JV-1 from his home phone number, the caller ID was in the name of FORDLEY's mother. When FORDLEY called JV-1 from his cell phone, the caller ID was in the name of FORDLEY's mother.

15. JV-1 engaged in verbal phone sex with FORDLEY at FORDLEY's request. In addition, FORDLEY asked JV-1 to send topless and nude photographs of herself to him.

16. JV-1 took a nude photograph of herself with her cellular phone in her mother's bedroom and sent it to FORDLEY via text message. FORDLEY responded, via text message, by saying she is gorgeous and beautiful with curves in all the right places. FORDLEY told JV-1, on the phone, that he "jerked off" to the picture.

17. FORDLEY also asked JV-1 to send him a topless photograph. In response, JV-1 took a photograph of herself in her mother's bedroom with her cell phone in front of the mirror and sent it to FORDLEY via text message. FORDLEY responded, via text message, by saying he wanted to "suck on them."

18. Using her cell phone, JV-1 also sent FORDLEY a photograph of herself, nude from the waist down, from behind and sent it to FORDLEY via text message. FORDLEY responded, via text message, by saying, "I want to fuck you so bad."

19. FORDLEY sent JV-1 two photographs of his penis via text message. FORDLEY included a message with one of the photographs of his penis saying that "I want to use this with

you” and “I want to have sex with you.” JV-1 stated that FORDLEY’s hand was on his penis in both pictures and something was depicted coming out of his penis in one of the pictures.

20. JV-1 deleted all of the photographs that FORDLEY sent to her.

21. According to JV-1, FORDLEY has an iPhone 4S and his cell phone number is (518) 495-0900. FORDLEY further identified his email address as mqs363@aol.com.

22. FORDLEY and JV-1 discussed meeting in person, but a specific plan was never put into place. In text messages and on the phone, FORDLEY offered to wire JV-1 money to purchase train or bus tickets to visit him in New York.

23. JV-1 last spoke with FORDLEY in early November 2014.

24. On November 10, 2014, a Facebook page was located for ETHAN FORDLEY at www.facebook.com/ethan.fordley. In that page, FORDLEY identified himself as being employed in carpentry and living in Albany, New York. JV-1 was shown a photograph that FORDLEY posted on his Facebook page and she identified that image as being the person with whom she had communicated.

25. On November 12, 2014, the cellular phone utilized by JV-1, phone number (508) 736-9612, was voluntarily provided to the Grafton, Massachusetts Police Department. Forensic examination has not, to date, managed to recover images or the content of any communications.

26. On November 20, 2014, a public records database query identified the service provider for (508) 736-9612, JV-1’s phone, as New Cingular Wireless (now owned by AT&T).

27. Further query of that database on November 20, 2014 identified (518) 495-0900, the number utilized by FORDLEY during the above noted communications with JV-1, as a New Cingular Wireless number assigned to FORDLEY’s mother in Albany, New York. On December 3, 2014, a public records database query provided further information as to

FORDLEY's mother, identifying her by name and revealing an address of 5 Haley Court, Albany, New York 12205, home telephone number (518) 453-8324.³ Ethan FORDLEY, year of birth 1991, was identified as a household member of 5 Haley Court, Albany, New York 12205.

28. I have obtained toll records from AT&T for the number assigned to JV-1's phone, (508) 736-9612. Consistent with what has been related by JV-1 concerning her phone contact with FORDLEY, those records reflect the following calls between JV-1's phone and both the home number of FORDLEY's mother, (518) 453-8324, and, the cell phone utilized by FORDLEY, (518) 495-0900:

- a. October 8, 2014 – (1) a call⁴ from JV-1's phone to (518) 495-0900, the cell phone utilized by FORDLEY, at approximately 3:26 p.m. EST (19:26 UTC)⁵ and which lasted under two minutes;

(2) a call at approximately 3:29 p.m. EST (19:29 UTC) from (518) 453-8324, the home number of FORDLEY's mother, to JV-1's phone and which lasted about 56 minutes;
- b. October 9, 2014 – (1) a call from JV-1's phone to (518) 495-0900, the cell phone utilized by FORDLEY, at 3:01 p.m. EST (19:01 UTC), and which lasted about one hour;
- c. October 10, 2014 – (1) a call from JV-1's phone to the (518) 495-0900, the cell phone utilized by FORDLEY, at 4:32 p.m. EST (20:32 UTC), and which lasted about eleven minutes;

³ As noted above and further described below, some calls to JV-1 occurred utilizing the phone assigned this number.

⁴ In many instances, the toll records reflect two calls made at the same time which are of approximately the same length. I interpret these as reflecting one call.

⁵ The AT&T records record times in Coordinated Universal Time (UTC).

- d. October 21, 2014 - (1) a call from JV-1's phone to (518) 495-0900, the cell phone utilized by FORDLEY, at 12:16 p.m. EST (16:16 UTC), and which lasted just under four minutes;
- e. October 23, 2014 – (1) a call from (518) 495-0900, the cell phone utilized by FORDLEY, to JV-1's cellphone at 5:15 p.m. EST (21:15 UTC), and which lasted only seconds;
- f. October 24, 2011 - (1) a call from JV-1's phone to (518) 495-0900, the cell phone utilized by FORDLEY, at 10:38 p.m. EST (2:38 UTC on 10/25), and which lasted just over one minute;

(2) a call from (518) 495-0900, the cell phone utilized by FORDLEY, at 10:38 p.m. (2:38 UTC on 10/25), and which lasted about twenty six minutes;

(3) a call from (518) 453-8324, the home number of FORDLEY's mother, to JV-1's phone at 11:04 p.m. (3:28 UTC on 10/25), and which lasted about forty three minutes;
- g. October 25, 2014 – (1) a call from JV-1's phone to (518) 495-0900, the cell phone utilized by FORDLEY, at 8:34 a.m. EST (12:34 UTC), and which lists a duration of 0 seconds;

(2) a call from JV-1's phone to (518) 495-0900, the cell phone utilized by FORDLEY, at 10:59 p.m. (2:59 UTC on 10/26), and which lasted about twenty eight minutes;
- h. October 26, 2014 - (1) a call from JV-1's phone to (518) 495-0900, the cell phone utilized by FORDLEY, at 8:43 p.m. EST (0:43 UTC on 10/27), and which lasted about thirty two minutes;
- i. October 27, 2014 - (1) a call from JV-1's phone to (518) 495-0900, the cell phone utilized by FORDLEY, at 12:20 p.m. EST (16:20 UTC), and which lists a duration of 0 seconds.

Interview of Ethan Fordley

29. On December 3, 2015, agents travelled to the SUBJECT PREMISES to Interview FORDLEY.

30. Briefly, FORDLEY agreed to speak to agents, and, in a recorded statement, admitted to conversing with JV-1 and to soliciting and obtaining pornographic images from JV-1.

31. FORDLEY identified an iPhone 4s, which I determined to be a Model A1387,ic 579c-e2430a, which he provided to agents, as the device upon which he had communicated with JV-1.

32. FORDLEY further admitted that he had conversed over the internet with other minor females, had solicited and obtained additional pornographic images from other minors, and that images and evidence of those chats would be found on a second phone, which he provided to agents. The second phone can be described as a Samsung Galaxy S5, Model Number SM6360T1.

33. FORDLEY further admitted that he had conversed over the internet with other minor females, had solicited and obtained additional pornographic images from other minors, and that images and evidence of those chats would be found on a laptop computer located in the home. The laptop can be described as an HP Laptop Model Number G6-1D60US.

34. Agents are presently at the SUBJECT PREMISES, awaiting the issuance of this warrant.

35. Based upon the foregoing, there is probable cause to believe that an iphone 4s, Model A1387,ic 579c-e2430a and the phone assigned the number (518) 495-0900 was used by FORDLEY to commit the TARGET OFFENSES, namely: to entice, persuade and induce JV-1 to engage in sexually explicit conduct for the purpose of creating child pornography; to engage

in verbal and text message communications seeking to persuade, induce and/or entice JV-1 to engage in unlawful sexual conduct; to engage in verbal and text message communications during which FORDLEY transmitted obscene images of his penis to JV-1.

36. Based upon the foregoing, there is also probable cause to believe that evidence of the TARGET OFFENSES will be found on other electronic devices capable of accessing the Internet, including the second FORDLEY telephone identified as a Samsung Galaxy S5, Model Number SM6360T1, and an HP Laptop Model Number G6-1D60US, which is presently located within the SUBJECT PREMISES, and which may have been used by FORDLEY to engage in online communications with other minors and which may contain pornographic images of those minors.

37. Persons who produce, possess, receive, distribute and advertise child pornography place significant value on images and videos of child pornography (and related materials). Since child pornography is illegal, it can be risky to obtain. Thus, individuals who produce, possess, receive, distribute and advertise child pornography are very unlikely to destroy or dispose of images once they are obtained. Indeed, it is well-established that individuals who produce, possess, receive, distribute and advertise child pornography hoard their images (and related materials) for many years, rarely, if ever, destroying them. This is particularly true today, when most child pornography is obtained via the Internet and can be easily stored in digital format on a computer or other data storage device. Accordingly, if an individual saves a digital image of child pornography on his computer, that image is likely to be present on that computer several years later. Indeed, even if the individual were to destroy the digital image (or attempt to destroy it), which is rare, it is very likely that the image would still be present on, and recoverable from, the subject's computer years later.

38. In addition to maintaining their images for long periods of time, persons who produce, possess, receive, distribute and advertise child pornography almost always maintain and possess their materials within a private location such as their home. In today's computer age, the majority of such images are likely to be maintained in digital form on a computer or other data storage device located in the subject's home. As described above, such images are likely to remain on a subject's computer or other data storage device for many years.

39. Based upon the facts described herein, there is probable cause to believe that FORDLEY has produced child pornography, attempted to entice or coerce or entice a minor to engage in unlawful sexual conduct and has transferred obscene materials to a minor. As described above, FORDLEY likely places great value on these images and maintains them on his computer or other data storage device in his home to this day.

40. Given the propensity of individuals who produce, possess, receive, distribute and advertise child pornography to store such images and/or videos within the privacy of their own homes, there is probable cause to believe that FORDLEY currently maintains evidence of the TARGET OFFENSES within the SUBJECT PREMISES.

COMPUTER AND DIGITAL EVIDENCE

41. Based on my knowledge, training, and experience, I know that electronic devices, such as cell phones, tablets, and computers can store information, pictures, and videos for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on such devices. This information can sometimes be recovered with forensics tools.

42. Based on my training and experience, and discussions with members of the FBI Computer Analysis Response Team (“CART”) and members of the HSI digital forensics squad, I know that a qualified computer specialist is required to properly retrieve, analyze, document and authenticate electronically stored data, and to prevent the loss of data either from accidental or deliberate programmed destruction. To do this work accurately and completely requires the seizure of: (1) all computer equipment and peripherals, which may be interdependent; (2) the software to operate the computer system(s); (3) the instruction manuals, which contain directions concerning the operation of the computer system(s) and software programs; and, (4) all internal and external data storage devices. Each of the seized items should be searched in a laboratory or controlled environment.

43. Searching computer systems and mobile electronic devices for criminal evidence is a highly technical process requiring expert skill and a significant amount of time. Indeed, computer specialists, using exacting data search protocols, must often recover hidden, erased, compressed, password-protected, or encrypted files in order to find evidence of criminal activity. Moreover, many commercial computer software programs save data in unique formats that are not conducive to standard data searches. This requires additional effort by specialists to review such data for evidence of a crime. Finally, many users try to conceal criminal evidence by storing files in random order with deceptive file names. This requires specialists to examine all of a user’s stored data to determine which particular files are relevant and within the scope of the search warrant. This process can take a substantial amount of time depending on the volume of data stored.

44. Because computer evidence is extremely vulnerable to tampering or destruction, both from external sources or from destructive codes imbedded in the system as "booby traps," a controlled environment is essential to a complete and accurate analysis.

45. Data storage devices, including but not limited to hard drives, diskettes and compact disks ("CDs"), can store the equivalent of thousands of pages of information. The majority of computers currently sold have, at a minimum, a 40 gigabyte hard drive, or larger, with an equivalent capacity in excess of 10,000,000 pages of typewritten, double spaced text.

46. Based on my training and experience, and discussions with members of CART and members of the HSI digital forensics squad, I know that many users of cellular phones, tablets and other mobile devices "sync" their mobile device to a computer and the cloud. This serves to provide convenient access to contacts, photographs, communications, and other data across electronic platforms and also serves to insure that information such as contact lists, photographs, videos, and other data will be preserved even if the mobile device is lost. In the process of syncing the device, images and/or videos can be transferred or saved to a home computer or cloud storage account. In addition, most peer-to-peer applications operate on numerous mobile and computer based platforms and can be utilized on both mobile devices and computers.

47. Through my training and experience I have discovered that private citizens and businesses are using electronic service providers who provide the service of storing data from anywhere there is service to the Internet, commonly known as "cloud" based storage. This allows the customer to connect to the server and view, alter, create, copy, and print the data from the remote server as if it was at the same location as the user. The user typically owns and

controls the data stored at the remote server while the electronic service provider owns the server on which the data is stored.

48. Law enforcement typically does not find out about the existence of the remote server until the service of the initial search warrant takes place. Law enforcement cannot access or view this cloud based data unless they know it exists and have access to a remote computer capable of connecting and authenticating to the user's cloud-based account. Witnesses and informants who have access to the data typically do not know where the data is stored either.

49. The server may be located in another city or state from the site of the initial service, making it difficult for law enforcement to preserve the evidence in a traditional manner. It takes hours and sometimes days to determine the location of the remote server and gather the details containing the specificity necessary for the issuance of a second search warrant. Depending on the size of the evidence, a suspect can delete it from a system within seconds using a smart phone or another Internet capable device away from the search warrant location. A forensic examiner often can recover evidence suggesting whether a computer (including a computer, cell phone or other Internet capable device) was used to access data which had been stored on a remote server in a cloud storage account. Such information is often maintained indefinitely until overwritten by other data.

50. For the reasons described in paragraphs 41-49 of this affidavit, it is necessary to seize all electronic devices, cellphones, smart phones, computers, data storage devices and related equipment located in the SUBJECT PREMISES as described in Attachment B. It is further necessary to search such equipment in a controlled environment, off-site. Given the potential for large quantities of data, a complete forensic examination of the seized items will take longer than fourteen days.

51. To the extent practical, if persons claiming an interest in the seized electronic devices so request, I will make available to those individuals copies of requested files (so long as those files are not considered contraband) within a reasonable time after the execution of the search warrant. This should minimize any impact the seizures may have on the device user's personal and/or business operations. In addition, as soon as practical, those items of hardware and software no longer required for the purpose of analysis or copying of items authorized to be seized, or for the preservation of the data and/or magnetic evidence, will be returned to the party from which they were seized, so long as such items do not constitute contraband.

52. Based on my training and experience and my discussions with members of CART and HSI digital forensics, I know that, in most cases, a trained computer specialist can retrieve deleted image files from a computer or other data storage device, including deleted images. Depending on the size of the computer or data storage device, deleted images can be retrieved for years after they have been deleted by the user. Thus, if a user possesses images or electronic correspondence, evidence of those images and/or electronic correspondence is likely to be present on his or her computer or other data storage device years later, regardless of whether the user has deleted or attempted to delete the images and/or electronic correspondence.

53. Based on my training and experience, and discussions with members of CART and members of the HSI digital forensics squad, I know that forensic evidence on a computer, smartphone, tablet, or other electronic device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

54. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

55. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer or phone is evidence may depend on other information stored on the device and the application of knowledge about how that device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

56. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

57. Based upon my training and experience, and my discussions with members of CART and HSI digital forensic squad, I know that when an iPhone, other smart phone, tablet or a digital camera is used to take a photograph or video, the device will often store information beyond the photograph itself. This “meta data” can include, the size of the file, its location on the device, the time and date of the photograph or video, GPS coordinates for where the photograph or video was taken, whether and when it has been accessed or modified, what device took the photograph or video, and other properties or data regarding the photograph or video.

58. Based on my training and experience, and discussions with members of CART and members of the HSI digital forensics squad, I know that modern smartphones, tablets, and other mobile devices, are equipped to access the Internet both through cellular data service and

through wireless Internet routers (“wi-fi”) in individual’s homes (or other locations that wi-fi is available). In fact, because wi-fi is almost always faster, modern mobile devices will often default to wi-fi to access the Internet when both cellular and wi-fi signals are available.


59. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of electronic devices and storage mediums consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

60. In addition to the more thorough off-site examination, FBI may also perform preliminary, on-site, forensic examinations of the cellular phones, computers and/or computer media to determine whether any of the items to be seized, are present on any electronic storage device on the premises. For the reasons previously stated, this preliminary on-site forensic evaluation cannot serve as a substitute for the complete, off site, forensic evaluation.

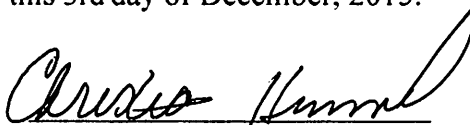
CONCLUSION

61. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence, fruits and instrumentalities of the TARGET OFFENSES will be found on an iphone 4s, Model A1387,ic 579c-e2430a, the phone assigned the numbers (518) 495-0900, and a Samsung Galaxy S5, Model Number SM6360T1 provided to law enforcement by Ethan FORDLEY. Additionally, there is probable cause to believe that evidence, fruits and instrumentalities of the TARGET OFFENSES will be found at 5 Haley Court, Albany, New York, including, but not limited to an HP Laptop Model Number G6-1D60US. Such evidence, fruits, and instrumentalities are more fully described in Attachment B attached hereto.

WHEREFORE, your affiant requests that this Court issue a Search Warrant for an iphone 4s, Model A1387,ic 579c-e2430a, the phone assigned the numbers (518) 495-0900 ,a Samsung Galaxy S5, Model Number SM6360T1 and any computers, computer equipment or computer storage media and electronic storage media located at 5 Haley Court, Albany, New York, including an HP Laptop Model Number G6-1D60US.


Chris Smith
Task Force Officere
Federal Bureau of Investigation

Subscribed and sworn to before me this 3rd day of December, 2015.


Hon. Christian F. Hummel
United States Magistrate Judge

ATTACHMENT A

PLACES AND ITEMS TO BE SEARCHED

The places and items to be searched are (A) 5 Haley Court, Albany, New York; and (B) any computers, computer equipment or computer storage media and electronic storage media located during the course of said searches, including, but not limited to, an iphone 4s, Model A1387,ic 579c-e2430a, the phone assigned the number (518) 495-0900, a Samsung Galaxy S5, Model Number SM6360T1, and an HP Laptop Model Number G6-1D60US.

5 Haley Court, Albany, New York is further described as the premises containing a single family ranch style residence that is lightish green in color. It has a two car attached garage with white doors that are located on the left of the home as viewed from the street. The residence has a white door and is depicted in the attached photograph.



ATTACHMENT B

Definitions

As used herein, the terms “records” and “information” include all items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term “device” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, gaming systems, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

Items to be Seized

All records relating to violations of the TARGET OFFENSES, production and attempted production of child pornography, in violation of 18 U.S.C. §2251; using of a means or facility of interstate commerce to induce, persuade and/or entice a minor to engage in unlawful sexual activity, in violation of 18 U.S.C. §2422(b), and using a means or facility of interstate commerce to transfer obscene materials to a minor, in violation of 18 U.S.C. §1470, those violations involving Ethan FORDLEY and occurring in or around October and November of 2014, including:

1. Any computer, cellphone, tablet, or other electronic device capable of accessing the Internet; including all electronic data or records within those items described in this Attachment;
2. An iphone 4s, Model A1387,ic 579c-e2430a; The phone assigned the number (518) 495-0900 and a Samsung Galaxy S5, Model Number SM6360T1.
3. The HP Laptop Model Number G6-1D60US.
4. The content of any communications between FORDLEY and any minor, including, JV-1, including, but not limited to, text messages, messaged photographs, and stored voicemails;
5. Any images of child pornography or images contained within communications between FORDLEY and any minor, including JV-1;

6. The stored history of calls made and received between FORDLEY and JV-1, or any other minor, on any phone seized pursuant hereto;

7. Digital photographs, and/or computer files and any other electronically stored visual depictions of images or video files sent between FORDLEY and any minor, including JV-1, along with all electronic metadata associated with those images or videos, and any hard copy or print out of such images;

8. Electronically stored contacts, such contact information for any minor, including JV-1, including but not limited to, the presence of such contact information in either a contacts file or in a drop down menu of previously emailed or contacted addresses in any electronic device;

9. Electronically stored user accounts and account passwords for any account for "www.poo.com;"

10. Records, documents, correspondence, notes, and/or any other materials relating to chats occurring on "www.poo.com," between FORDLEY and JV-1;

11. Records evidencing the use of any electronic device to communicate with the www.poo.com website including:

- a. all user account information submitted to www.poo.com by FORDLEY;
- b. the content of all emails or other communications from administrators of that website to FORDLEY and all information relating to where such messages were sent, and from whom they were sent;

12. Records or other items that evidence ownership or use of computer(s) or other electronic devices or equipment including user attribution information, sales receipts, registration data, electronically stored correspondence, communication, and photographs;

13. Electronically stored records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, and records of user-typed web addresses;

14. Evidence of ownership and/or residency at 5 Haley Court, Albany, New York;

15. All camera equipment, including but not limited to, digital and video cameras, web cameras, camera phones, and digital memory cards, and any electronic device capable of taking digital photographs, and any evidence of ownership of such devices such as billing records, evidence of purchase, or user attribution information;

16. Routers, modems, and network equipment used to connect computers or other devices to the Internet; Electronically stored records of Internet Protocol addresses used;

17. For any computer, device, or storage medium whose seizure is otherwise authorized by this warrant, and any computer, device, or storage medium that contains, or in which is stored, records or information that is otherwise called for by this warrant (hereinafter, "DEVICE"):

- a. evidence of who used, owned, or controlled the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the DEVICE of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICE;
- f. evidence of the times the DEVICE was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the DEVICE;
- h. the software used to operate the computer(s), and any compact disks (CDs), zip disks, floppy disks, digital video disks (DVD), memory cards, thumb drives, and other magnetic storage devices;
- i. documentation and manuals that may be necessary to access the DEVICE or to conduct a forensic examination of the DEVICE;
- j. records of or information about Internet Protocol addresses used by the DEVICE;
- k. records of or information about the DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- l. contextual information necessary to understand the evidence described in this attachment.